NUREG-0800
(Formerly NUREG-75/087)

U.S. NUCLEAR REGULATORY COMMISSION

STANDARD REVIEW PLAN

OFFICE OF NUCLEAR REACTOR REGULATION

Section 7.5. Information Systems Important to Safety

Review Responsibilities

Primary — Instrumentation and Controls Branch (HICB)

Secondary — None

I. Areas of Review

This SRP section describes the review process and acceptance criteria for those instrumentation and control (I&C) systems that provide information to the plant operators for: (1) assessing plant conditions, safety system performance and making decisions related to plant responses to abnormal events; and (2) preplanned manual operator action related to accident mitigation. The information systems reviewed using this section also provide the necessary information from which appropriate actions can be taken to mitigate the consequences of anticipated operational occurrences. The systems reviewed using Section 7.5 of the SRP include the following:

- Post-accident monitoring (PAM) systems.

- Bypassed or inoperable status indication (BISI) for safety systems.

- Plant annunciator (alarm)[1] systems

- Safety parameter display system (SPDS).

- Information systems associated with the emergency response facilities (ERF) and nuclear data link (NDL).

For SPDS, ERF, and NDL, the HICB review is limited to the system interface with the plant control and protection systems. Functional performance of those systems, as well as functional aspects of other I&C systems — such as radiation monitoring, fire detection, and the information systems for environs conditions during and following an accident — are addressed in the review of other sections of the safety analysis report (SAR).

The objectives of the review are to confirm that the information systems important to safety satisfy the requirements of the acceptance criteria and guidelines applicable to these systems, and that they will provide the information to ensure plant safety during all plant conditions for which they are required.

SRP Section 7.0 describes the coordination of reviews, including the information to be reviewed and the scope required for each of the different types of applications that the Office of Nuclear Reactor Regulation (NRR) may review. Refer to that section for information regarding how the areas of review are affected by the type of application under consideration and for a description of coordination between HICB and other branches.

II. Acceptance Criteria

The acceptance criteria and guidelines applicable to information systems important to safety are identified in SRP Section 7.1. The review of Section 7.1 of the SAR confirms that the appropriate acceptance criteria and guidelines have been identified for these systems. The review of the information systems important to safety in this section of the SAR confirms that these systems conform to the requirements of the acceptance criteria and guidelines.

Acceptance criteria for the review of the information systems important to safety are based on meeting the relevant requirements of the following regulations.

1. Acceptance criteria applicable to post-accident monitoring systems

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For post-accident monitoring systems isolated from the protection system, the only applicable requirement from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

[1]For the purposes of this section, the annunciator system is considered to consist of sets of alarms (which may be displayed on tiles, video display units, or other devices) and sound equipment; logic and processing support, and functions to enable operators to silence, acknowledge, reset, and test alarms.

10 CFR 50.34(f), "Additional TMI-Related Requirements," or equivalent TMI action plan requirements imposed by Generic Letters. The following portions of this part apply to PAM systems.

(2)(xii), " Auxiliary Feedwater System Flow Indication" (applicable to PWRs only).

(2)(xvii), "Accident Monitoring Instrumentation."

(2)(xviii), "Inadequate Core Cooling Instrumentation."

(2)(xix), "Instruments for Monitoring Plant Conditions Following Core Damage."

(2)(xx), " Power for Pressurizer Level Indication" (applicable to PWRs only).

(2)(xxiv), "Central Reactor Vessel Water Level Recording" (applicable to BWRs only).

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 2, "Design Basis for Protection Against Natural Phenomena" (applicable only to channels classified as Category 1 or 2 in Reg. Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident").

General Design Criterion 4, "Environmental and Missile Design Basis" (applicable only to channels classified as Category 1 or 2 in Reg. Guide 1.97).

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

2. Acceptance criteria applicable to bypassed and inoperable status indication

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For BISI that are isolated from the protection system, the only applicable requirements from ANSI/IEEE Std 279 are item 4.7.2, "Isolation Devices," and 4.13, "Indication of Bypasses."

10 CFR 50.34(f)(2)(v), "Additional TMI-Related Requirements" - bypass and inoperable status indication, or equivalent TMI action plan requirements imposed by Generic Letters.

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 24, "Separation of Protection and Control Systems."

3. Acceptance criteria applicable to annunciator systems

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations." For annunciators that are isolated from the protection system, the only applicable requirements from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 13, "Instrumentation and Control."

General Design Criterion 19, "Control Room."

General Design Criterion 24, "Separation of Protection and Control Systems."

Additional acceptance criteria applicable to ALWR annunciator systems

Staff Requirements Memorandum (SRM), "SECY-93-087 — Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," Item II.T, "Control Room Annunciator (Alarm) Reliability." This SRM states:

> "... the alarm system for ALWRs should meet the applicable EPRI requirements for redundancy, independence, and separation. In addition, alarms that are provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions, shall meet the applicable requirements for Class 1E equipment and circuits."

4. Acceptance criteria applicable to the HICB review of SPDS, ERF information systems, and NDL information systems

10 CFR 50.55a(a)(1), "Quality Standards."

10 CFR 50.55a(h), "Protection Systems," requires compliance with ANSI/IEEE Std 279. For SPDS, ERF information systems, and NDL information systems isolated from the protection system, the only applicable requirement from ANSI/IEEE Std 279 is item 4.7.2, "Isolation Devices."

General Design Criterion 1, "Quality Standards and Records."

General Design Criterion 24, "Separation of Protection and Control Systems."

5. Additional criteria applicable to information systems important to safety proposed for design certification under 10 CFR 52

10 CFR 52.47(a)(1)(iv), "Resolution of Unresolved and Generic Safety Issues."

10 CFR 52.47(a)(1)(vi), "ITAAC in Design Certification Applications."

10 CFR 52.47(a)(1)(vii), "Interface Requirements."

10 CFR 52.47(a)(2), "Level of Detail."

10 CFR 52.47(b)(2)(i), "Innovative Means of Accomplishing Safety Functions."

6. Additional acceptance criteria applicable to information systems important to safety proposed as part of combined license applications under 10 CFR 52

10 CFR 52.79(c), "ITAAC in Combined License Applications."

Section 7.1, Table 7-1, and Appendix 7.1-A list standards, regulatory guides, and branch technical positions that provide information, recommendations, and guidance that describe a basis acceptable to the NRC staff for implementing the relevant requirements of the NRC regulations identified above.

III. Review Procedures

Section 7.1 describes the general procedures to be followed in reviewing any I&C system. Section 7.5 highlights specific topics that should be emphasized in the review of information systems important to safety.

The systems addressed below may be implemented either as stand alone systems or integrated as part of other systems. If the information systems are not isolated from the protection systems, they should also be evaluated according to the criteria in Section 7.2 or 7.3, as appropriate.

Other information systems (for example, plant computer and severe accident monitoring) may be included in the review. The acceptance criteria for such systems depend on the function of the system and the applicable design criteria.

Any exceptions or deviations to a post-accident monitoring system designed to satisfy Reg. Guide 1.97 should be identified in the SAR. This includes acceptable deviations and clarifications identified in BTP HICB-10.

The review should include an evaluation of the information systems design against the guidance of ANSI/IEEE Std 279, or Reg. Guide 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems" (which endorses IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"), depending upon the applicant/licensee's commitment regarding these design criteria. This procedure is detailed in Appendix 7.1-B for ANSI/IEEE Std 279 and in Appendix 7.1-C for IEEE Std 603. The procedures in Appendices 7.1-B and 7.1-C address specific design requirements.

The reviewer should consider the overall information system functions on a system level. The design should be compatible with the SAR Chapter 15 design bases accident analyses, and operating procedures as well as applicable guidance of ANSI/IEEE Std 279 or IEEE Std 603.

The review should also consider the guidance provided in NUREG-0737, Supplement 1, "Clarification of TMI Action Plan Requirements — Requirements for Emergency Response Capability," with respect to PAM, ERF, and SPDS.

The information systems review should address the topics identified as applicable in Table 7-1. Appendix 7.1-A describes review methods for each topic. Certain guidance documents identified in Parts 3 and 4 of Table 7-1 apply only to BISI or PAM, but not both. The guidance documents that are not applicable to a specific system are identified below.

Major design considerations that should be emphasized in the review of the information systems important to safety are identified below.

1. Recommended review emphasis for PAM

- Conformance with Reg. Guide 1.97 and BTP HICB-10.

- Use of digital systems — See Appendix 7.0-A.

- Emergency operating procedures (EOP) action points — A basis should be provided for EOP action points that accounts for measurement uncertainties. Draft Reg. Guide DG-1045, the proposed revision 3 to Reg. Guide 1.105, "Instrument Spans and Setpoints," provides acceptable guidance for establishing these uncertainties.

- Monitoring for severe accidents —The accident monitoring instrumentation should be demonstrated to perform their intended function for severe accident protection. They need not be subject to additional 10 CFR 50.49 environmental qualification requirements. However, they should be designed so there is reasonable assurance that they will operate in the severe-accident environment for which they are intended and over the time span for which they are needed.

2. Recommended review emphasis for BISI

- Scope of BISI indications — As a minimum BISI should be provided for the following systems:

  – RTS and ESFAS — See Appendix 7.1-B item 14 and Appendix 7.1-C item 13.

  – Interlocks for isolation of low-pressure systems from the reactor coolant system — See BTP HICB-1.

  – ECCS accumulator isolation valves — See BTP HICB-2.

  – Controls for changeover of RHR from injection to recirculation mode — See BTP HICB-6.

- Conformance with Reg. Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."

- Independence — See Appendix 7.1-B item 8 and Appendix 7.1-C item 24. The indication system should be designed and installed in a manner which precludes the possibility of adverse effects on plant safety systems. Failure or bypass of a protective function should not be a credible consequence of failures occurring in the indication equipment, and the bypass indication should not reduce the required independence between redundant safety systems.

- Use of digital systems — See Appendix 7.0-A.

3. Recommended review emphasis for annunciator systems

- Reliability — The applicant/licensee should justify that the degree of redundancy, diversity, testability, and quality provided in annunciator systems is adequate to support normal and emergency operations. Appendix 7.1-C item 20 provides guidance on the evaluation of safety system reliability that may be used in evaluating the reliability of annunciator systems.

- Use of digital systems — See Appendix 7.0-A.

- Independence (isolation between safety systems and other systems) — See Appendix 7.1-B item 8 and Appendix 7.1-C item 24.

Additional items for emphasis for ALWR annunciator systems

- Redundancy — Redundant alarm systems should be provided. These redundant systems need not comply with the single failure criterion, but independence between the redundant systems should be equivalent to that provided between redundant channels of the protection systems. See Appendix 7.1-B item 7 and Appendix 7.1-C item 11.

- Self-test provisions — See BTP HICB-17. The surveillance test portions of this BTP are not applicable.

- Compliance with IEEE Std 279 — Alarms that are provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions should be reviewed against the guidance of Reg. Guide 1.153. See Appendix 7.1-C.

4. Recommended review emphasis for SPDS, ERF information systems, and NDL information systems

- Independence (isolation between safety systems and other systems) — See Appendix 7.1-B item 8 and Appendix 7.1-C item 24.

In each safety review, the reviewer should determine the elements of the design that require additional review emphasis. Typical reasons for such a non-uniform emphasis are the introduction of new design features or the utilization in the design of features previously reviewed and found acceptable. However, in all cases, the review must be sufficient to conclude conformance to the acceptance criteria, i.e., the requirements of the Code of Federal Regulations.

IV. Evaluation Findings

The Staff verifies that sufficient information has been provided and the review supports the following conclusions as stated in the SER:

The NRC staff concludes that the designs of the information systems important to safety are acceptable and meet the relevant requirements of General Design Criteria (GDC) 1, 2, 4, 13, 19, and 24, and 10 CFR 50.34(f), 10 CFR 50.55a(a)(1), and 10 CFR 50.55a(h).

The Staff conducted a review of the information systems important to safety for conformance to the guidelines in the regulatory guides and industry codes and standards applicable to these systems. The Staff concluded that the applicant/licensee adequately classified and identified the guidelines applicable to these systems. Based upon the review of the system design for conformance to the guidelines, the Staff finds that the systems conform to the guidelines applicable to these systems. Therefore, the Staff finds that the requirements of GDC 1 and 10 CFR 50.55a(a)(1) have been met.

The review included the identification of those systems and components for the information systems important to safety that are designed to survive the effects of earthquakes, other natural phenomena, abnormal environments, and missiles. Based upon the review, the Staff concludes that the applicant/licensee has identified those systems and components consistent with the design bases for those systems. Sections 3.10 and 3.11 of the SER address the qualification programs to demonstrate the capability of these systems and components to survive these events. Therefore, the Staff finds that the identification of these systems and components satisfies the requirements of GDC 2 and 4.

The non-safety portions of information systems important to safety are appropriately isolated from safety systems, including the safety portions of the information systems. Therefore, the Staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 5.55a(h) and the requirements of GDC 24.

The instrumentation provided for monitoring severe accident conditions has been designed to operate in the severe-accident environment for which they are intended and over the time span for which they are needed. Therefore, the Staff finds that the severe accident monitoring instrumentation satisfies the requirements of GDC 2 and 4.

The post-accident monitoring system conforms to the guidelines for the instrumentation to access plant conditions during and following an accident provided in Reg. Guide 1.97. The redundant information systems conform to the guidelines for the physical independence of electrical systems provided in Reg. Guide 1.75. The instrument spans and EOP action points were established in accordance with the guidelines of Draft Reg. Guide DG-1045. The environmental monitoring system provided to protect the safety instrument sensing lines from freezing conforms to the guidelines of Reg. Guide 1.151, position 5. The post-accident monitoring system includes appropriate variables. The range and accuracy of the instrument channels for these variables are consistent with the plant safety analysis. The post-accident monitoring system includes appropriate variables for monitoring severe accident conditions. The variables monitored and the range and accuracy of instrumentation provided to monitor these variables is consistent with the severe accident analysis. Therefore, the staff finds that the post-accident monitoring system meets the requirements of GDC 13 and 19.

The post-accident monitoring system includes the following functions required by 10 CFR 50.34(f): [feedwater system flow indication[2]], accident monitoring instrumentation, inadequate core cooling instrumentation, instruments for monitoring plant conditions following core damage, [central reactor vessel water level recording[3]]. Additionally, the power supply for the PAM pressurizer level indication complies with the requirements of 10 CFR 50.34(f)(xx) [applicable to PWRs only]. Therefore, the Staff concludes that the instrumentation systems important to safety satisfy the requirements of 10 CFR 50.34(f), Subparts xii, xvii, xviii, xix, xx, and xxiv.

The Staff reviewed the systems for which a bypassed or inoperable status is indicated in the control room. The Staff finds that the bypass indications will give the operators timely information and status reports so the operators can mitigate the effects of unexpected system unavailability. The bypass indications satisfy the guidelines of Reg. Guide 1.47. Therefore, the Staff concludes that the BISI functions satisfy the applicable requirements of 10 CFR 50.55a(h) and 10 CFR 50.34(f)(2)(v).

The Staff reviewed the control room annunciator systems and finds that these systems are sufficiently reliable to support normal and emergency plant operations. [Redundant annunciator systems are provided and the independence of these redundant systems complies with the independence requirements of IEEE Std 279 Section 4.6 OR IEEE Std 603 Section 5.6. Alarms provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions comply with the guidance of IEEE Std 603.] Therefore, the Staff concludes that the annunciator systems satisfy the requirements of [the SRM on SECY-93-087 item II.T,] GDC 13 and 19.

Based upon the above items, the Staff finds that the information systems satisfy the requirements of GDC 13 for monitoring variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions. Further, the Staff finds that conformance to GDC 13 and the applicable guidelines satisfies the requirements of GDC 19 with respect to information systems provided in the control room from which actions can be taken to operate the unit safety under normal conditions and to maintain it in a safe condition under accident conditions.

The safety parameter display system, the information systems associated with the emergency response facilities, and the nuclear data link, non-safety portions of PAM, non-safety portions of BISI, and non-safety portions of the annunciator systems are appropriately isolated from safety systems. Electrical isolation devices were qualified in accordance with the guidance of BTP HICB-11. Therefore, the staff concludes that the isolation of these systems from safety systems satisfies the requirements of 10 CFR 50.55a(h) and GDC 24.

The applicant/licensee has also incorporated in the system design the recommendations of TMI task action plan items [identify item number and how implemented] that the Staff has reviewed and found acceptable.

In the review of the information systems important to safety, the Staff examined the dependence of these systems on the availability of essential auxiliary systems. Based on this review and coordination with those having primary review responsibility of EAS systems, the Staff concludes that the design of the information systems important to safety is compatible with the functional requirements of EAS systems.

[2]Applicable to PWRs only.

[3]Applicable to BWRs only.

Note: the following finding applies only to systems involving digital computer-based components.

Based on the review of software development plans and the inspections of the computer development process and design outputs, the Staff concludes that the computer systems meet the guidance of Reg. Guide 1.152. Therefore, the special characteristics of computer systems have been adequately addressed, and the Staff finds that the information systems important to safety satisfy these requirements of GDC 1.

Note: the following findings apply only to applications under 10 CFR 52.

The design of the information systems important to safety appropriately addresses the applicable unresolved and generic safety issues. Therefore, the Staff finds that the information systems important to safety satisfy the requirements of 10 CFR 52.47(a)(1)(iv).

The review of the information systems important to safety examined the proposed inspections, tests, analyses, and acceptance criteria (ITAAC). Based upon the review and coordination with those having primary responsibility for ITAAC, the Staff concludes that if the inspections, tests, and analyses are performed and the acceptance criteria are met, the plant will operate in accordance with the [design certification OR combined license]. Therefore, the Staff finds that the information systems important to safety satisfy the requirements of [10 CFR 52.47(a)(1)(vi) OR 10 CFR 52.79(c)].

The application for design certification does not seek certification for the following portions of the information systems important to safety [insert list]. Based upon review of the completed safety analysis, the Staff finds that the requirements for these portions of the design were sufficiently detailed. Therefore, the Staff finds that the design of the information systems important to safety satisfies the requirements of 10 CFR 52.47(a)(1)(vii).

The information systems important to safety contain the following elements that differ significantly from evolutionary changes from light water reactor designs of plants that have been licensed in commercial operation before April 18, 1989. [Insert list.] Based upon the review of [analysis OR test programs OR operating experience] the Staff concludes that the performance of these features has been demonstrated; interdependent effects among the safety features are acceptable; sufficient data exist to assess the analytical tools used for safety analysis; and the scope of the design is complete except for site-specific elements. Therefore, the Staff finds that the information systems important to safety satisfy the requirements of 10 CFR 52.47(b)(2)(i).

Based upon an initial review of the scope and content of the material submitted by the applicant, and completed review with respect to the technical items above, the Staff finds that the application contained appropriate detail about the information systems important to safety design to satisfy the requirements of 10 CFR 52.47(a)(2).

Note: the following conclusion is applicable to all applications.

The conclusions noted above for the information systems important to safety are applicable to all portions of the systems except for the following, for which acceptance is based upon prior NRC review and approval as noted. [List applicable system or topics and identify references.]

V. Implementation

Except in those cases in which the applicant/licensee proposes an acceptable alternative method for complying with specified portions of the NRC's regulations, the method described herein will be used by the NRC staff in its evaluation of conformance with NRC regulations.

VI. References

ANSI/IEEE Std 279-1971. "Criteria for Protection Systems for Nuclear Power Generating Stations."

Draft Regulatory Guide DG-1045. Proposed Revision 3 to Regulatory Guide 1.105, "Instrument Setpoints for Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997.

IEEE Std 603-1991. "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

NUREG-0737 Supplement 1. "Clarification of TMI Action Plan Requirements — Requirements for Emergency Response Capability." January 1983.

Regulatory Guide 1.151. "Instrument Sensing Lines." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1983.

Regulatory Guide 1.152. "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.153. "Criteria for Power, Instrumentation, and Control Portions of Safety Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1996.

Regulatory Guide 1.47. "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1973.

Regulatory Guide 1.75. "Physical Independence of Electrical Systems." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1978.

Regulatory Guide 1.97. "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1983.

Staff Requirements Memorandum on SECY-93-087. "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." July 15, 1993.